WEAPONS OF MASS EFFECT

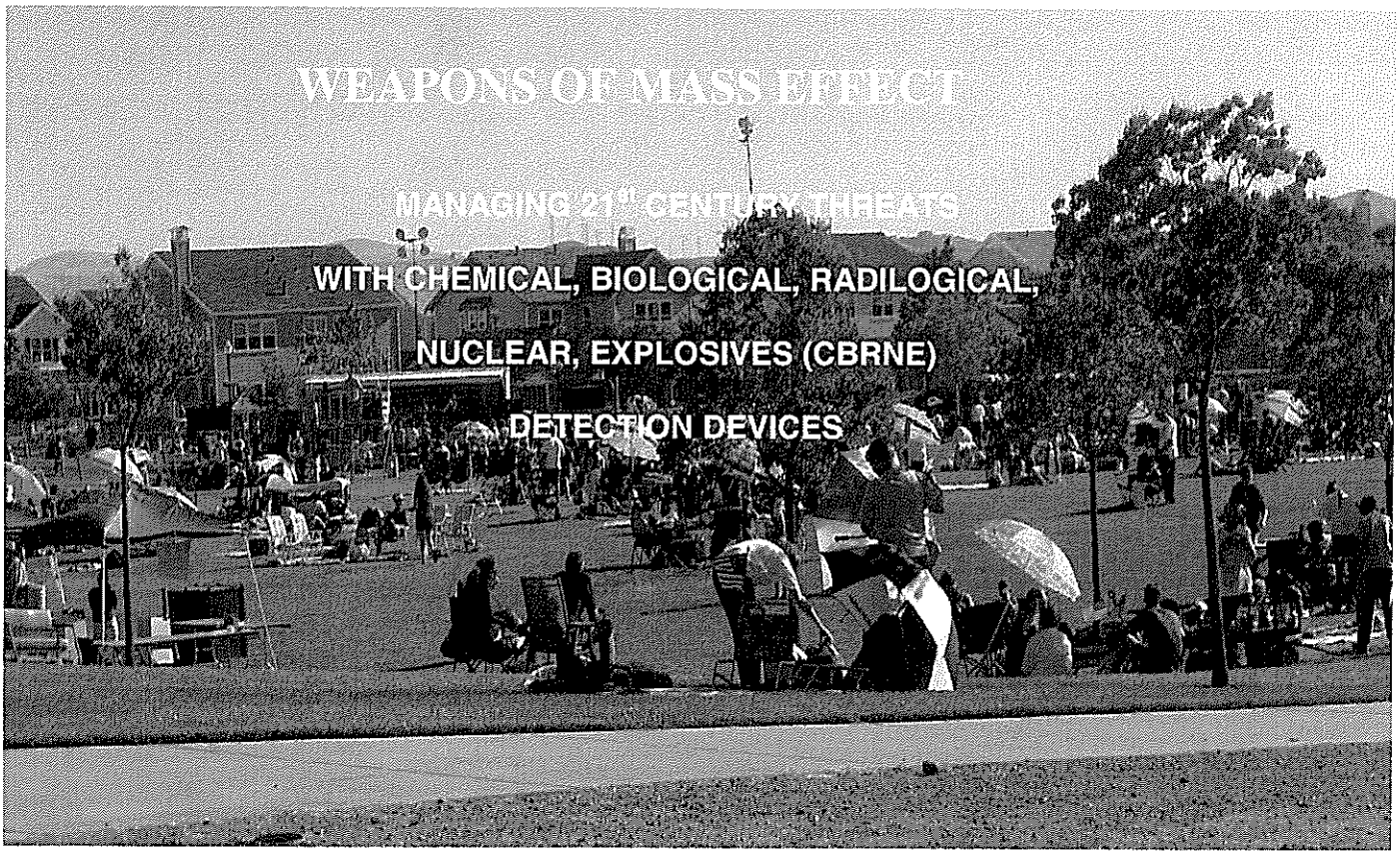
MANAGING 21st CENTURY THREATS WITH CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, EXPLOSIVES (CBRNE) DETECTION DEVICES

JOURNAL ARTICLE

LT. SCOTT TRUDEAU
LIVERMORE POLICE DEPARTMENT

COMMAND COLLEGE CLASS 39
PEACE OFFICER STANDARDS AND TRAINING
SACRAMENTO, CALIFORNIA

SEPTEMBER 2006



"The ability to unleash mass sickness, death, and destruction today has reached a far greater order of magnitude as the new millennium begins."

Former Defense Secretary William Cohen- 2000

The newest challenge we face in the law enforcement profession is unlike any other we have seen before. Incident planning and event intelligence in conventional times were straightforward. The local criminal element had a face, and in many cases a known, predictable method of operation that could be detected or omitted from the event. Terrorism has no face, and more importantly no predictable method of attack on an objective or target. When and who will be next? How will Law Enforcement prepare and prevent these acts before they injure and kill many innocent citizens?

Our communities not only expect us to meet this challenge, they will demand we take on all measures of prevention as the number of these events increase around the globe. Thus, our evolving mission will require that we have an understanding not only of our new role in this process, but a thorough understanding of how we will integrate new and emerging anti-terrorism plans and Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) detection technologies into our standard operation plans.

Historical Perspective

Traditionally we think of Weapons of Mass Destruction (WMD) as explosive devices which, aside from the impact of the explosion itself, spread radiation. We tend to overlook chemical weapons such as nerve agents, choking agents and blister agents; any of which may cause discomfort, illness or death. Additionally, we may be dealing with biological weapons that are viral; toxin or fungi based and can be delivered via a wide range of methods. Expanding on the theme of this myriad approach to possible devastation to people as well as the environment is an emerging description when discussing the overall impact of these devices on the general public: Weapons of Mass Effect (WME).

WME applications can be packaged and delivered in just about any manner imaginable. Discouraging or preventing the use of these devices must go beyond traditional methods such as target hardening and intelligence gathering. Our employees must be hyper vigilant, and technologically prepared to battle these 21st century threats. By implementing WME sensor technologies, we can begin to identify threats before they are deployed and take advantage of perhaps the most effective means by which to detect and respond to acts of terror against our citizenry.

The history of Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) Sensor use within the law enforcement profession is short term, and thus far has been limited to those larger metropolitan agencies seen as potential terrorist targets. Many of these agencies have only been exposed to these devices as a result of being in close proximity to private R&D companies wishing to test and promote their devices. For

most agencies, there is no specific plan for CBRNE detection, and more often than not, plans for chemical or biologic detection fall into the non-technical realm often referred to as the "blue canary" method of detection. In other words, most agencies have not considered, tested, purchased or deployed detection devices, and have traditionally relied on personnel to "respond" "observe" and "report" on situations such as chemical spills or hazardous gas release events.

Without proper planning and organizational change, CBRNE detection will more than likely fall into the same method of response, playing into the human tendency only to invest in preventative measures for calamities only after they have been personally experienced.[1] Beyond the obvious need for such devices, though, it is essential for law enforcement to develop incident management plans and identify innovative response approaches that can incorporate their use.

Historically, law enforcement has been slow to respond to change, and with rare exception, looks outside of the profession for proactive response to environmental, political, and technological changes. Law enforcement hasn't typically had the means to obtain new and cutting edge technology, often due to limits of funding or a lack of political will by elected officials seeking to balance competing concerns. The private sector hasn't had the same restrictions and thus has been able to move forward at a faster pace than law enforcement.

---

1. Levenson, N.G. 1995 *Safeware*: System Safety and Computers. Addison-Wesley.

During the past few years, however, law enforcement has had some success moving to address CBRNE response-related issues.

Washington D.C.

Early in 2003, Washington D.C. Metro Police began installation of the nation's first permanent detection systems to enhance any response to chemical attacks on a public place or venue. This system, developed by scientists at Sandia National Laboratory, merges computer-aided chemical monitoring with simultaneous closed circuit video monitoring. They've developed both a "liquid-phase" system, which can identify bio-toxins, viruses and bacterial agents, and a two gas-phase system used for detecting chemical warfare agents and a selection of toxic industrial chemicals, as well as explosives and organic solvents.[2] Computers in the D.C. Metro Police command center can monitor and map the release of toxins during the situation; first responders have the same information on their laptops. This information can be used to direct passengers to "cold zones" that are safe and can facilitate the extraction of passengers from the facility.[3]

Livermore, CA

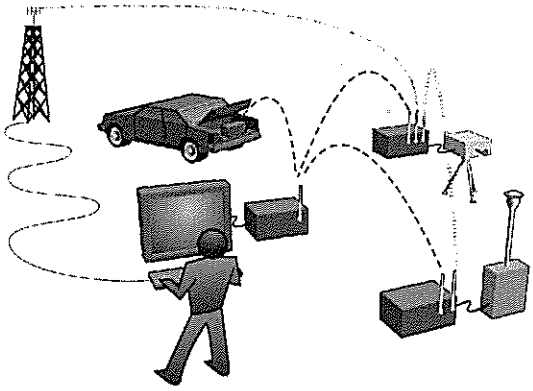
Another example of ongoing CBRNE testing by law enforcement took place in July 2004, when Sandia National Laboratories partnered with the Livermore, California

[2] Sandia seeks commercialization partners for hand-held chemical analysis and detection system."MicroChemLab" device serves as homeland security tool for first-line responders and offers variety of other applications.: http://www.sandia.gov/news-center/news-releases/2003/mat-chem/chempartners.html

[3] Sandia Sensors Guard D.C. Labs protect D.C. Metro: http://www.ca.sandia.gov/news/2003-news/030316news.html

Police Department to test new R&D high-tech sensory systems. The two agencies deployed a networked series of environmental detectors and high-resolution cameras during a Fourth of July celebration in Livermore to assess the abilities of biological, chemical and radiological sensors. The sensors were connected to a central command post via an encrypted and wireless transmission, allowing police and fire managers to remotely monitor the data.

Sensor Management Architecture (SMA)



An intelligent, rapidly deployable sensor integration and management architecture supporting operations and simulation

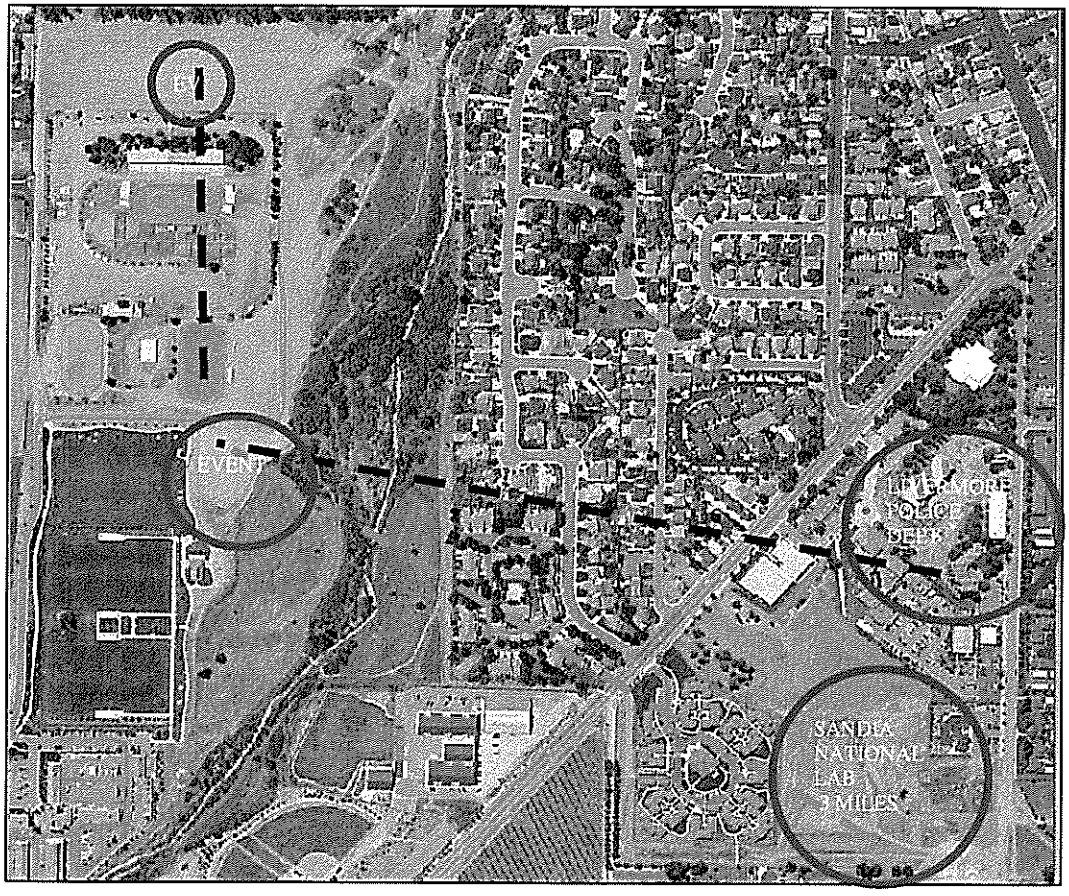
Livermore Police Department/Sandia National Laboratory 2004 [4]

The author participated in this deployment, assessing the ability to integrate this technology into the existing mobile and fixed command post structure. During Livermore's 4th of July celebration, our agency and Sandia's personnel placed multiple environmental detectors and cameras (as well as mobile sensor monitors and wireless data processing equipment) at various points in the celebration locale. While we did not have any detection alerts during the exercise, we were able to easily fit the equipment

[4] Sandia Labs: http://ca.sandia.gov/news/2004news/080504news.html

within our mobile command post structure, as well test the ease of use of the wireless data equipment with the personnel deployed at the event. We were also able to simultaneously send the wireless data to a simulated (fixed) command post set up within the Livermore Police Department, and the Sandia National Laboratory, located one and three miles respectively from the event. The results where exciting when you realize the many positive results an agency would have in enhancing the public's security and safety during a large public gathering.

2004 Deployment locations included the coverage of the event location, the Livermore Rodeo Grounds, Robertson Park, the Livermore Police Headquarters, and Sandia National Laboratories.



Livermore Police Department/Sandia National Laboratory 2004

The Super Bowl

In February 2006, the Michigan National Guard utilized handheld and fixed sensors to monitor fans attending Super Bowl XL at Ford Field in Detroit. Each of the devices was linked via a wireless network, which provided real time data to a centralized command post to monitor potential threats. Additionally, this system allowed for secure data to be monitored via web sites for monitoring at any location around the world. The sensor technology being used by the Michigan National Guard for Super Bowl XL was part of a field test for the U.S. Army's Tank and Automotive Research, Development and Engineering Center (TARDEC). The goal for testing this technology was to assess ways in which to link sensors, military personnel, vehicles and other equipment using high-speed wireless networks for instant and reliable communications.[5] While we know there were more than 65,000 attendees at the Super Bowl, the actual numbers of fans that were scanned are not available. The testing was done without media fanfare, and the specific results were not disclosed on this "work in progress."

As with any plan to counter an unusual occurrence, we must be flexible and capable of rapid response and operational deployment of resources. To combat and deter the use of CBRNE by terrorist, we must consider using CBRNE Sensor technologies. The ability to effectively monitor high-profile special events involving dignitaries, political gatherings, or any event where large crowds will gather will be of significant benefit to the law enforcement profession. Based on the success of these three examples, one can

---

5 Super Bowl security to use sensor fusion to fight WMD threats
The Michigan National Guard will be field testing devices for the U.S. Army
Todd Weiss Computerworld Magazine Feb. 2006

already see these devices are not intrusive, and public acceptance will come from the increased speed at which they can now access venue sites without the need for inspection of clothing or personal items.

Planning for Use and Deployment

There can be little debate over the need for CBNRE sensors as a part of the police arsenal to combat potential acts of terror. One can easily visualize these sensors being deployed routinely by law enforcement in the very near future. Whether at a sporting event as tested this year at the Super Bowl, or a Broadway theater show or even a tourist location such as the Smithsonian Museum in Washington D.C., there are endless possibilities for the use of the equipment. The public has become accustomed to video surveillance technology in various aspects of their day-to-day activities in a number of public and business locales. CBRNE will be a natural accompaniment to systems already in place.

We already have companies marketing wireless Toxic Gas/Radiation systems that can monitor threats up to 2 miles away from a public safety command post. Costs run from $50,000 for a basic system up to $100,000 or more for a custom system. Training necessary to operate such systems is not complex, and can be completed in as little as sixteen hours for field personnel. There are a number of potential funding sources for these systems. Locally public service organizations within the community, private business as well as State and Federal grants will aid the local jurisdiction to acquire the technology and fund necessary training. Additionally, Department of Homeland Security (DHS) grant money may be utilized through cooperative acquisition processes

established between cities and the respective county sheriff's office. With these options, it is doubtful the upfront cost would displace general fund money needed for other agency activities. Perhaps the best source for funding and equipment comes through the Department of Homeland Security through its Commercial Equipment Direct Assistance Program (CEDAP). CEDAP is operated by the DHS' Office of State and Local Government Coordination and Preparedness to help smaller communities that have not received direct federal homeland security grants. In 2005 the department awarded technology valued at $8 million to 697 jurisdictions under the program. The CEDAP program provides the technology, as well as technical assistance and can provide the personnel training.

Without question, some of the biggest challenges lie in the management and response to the information gleaned from the sensors once they are deployed. Who will dictate the use and initial deployment? How will the devices be monitored and subsequently interpreted by law enforcement? Will false-positive or false-negative reactions undermine the process? Do we respond en masse to any CBRNE detections from these devices? Will our City Managers, City Councils and citizens support and understand the multitude of issues that will come from the deployment of CBRNE Sensor's? With the inevitable use of these devices, and the multitude of questions surrounding their use, how will law enforcement deploy and manage these new technologies in the future?

Politics

Law enforcement agencies considering the use of CBRNE devices must first realize the need to gain public acceptance and understanding of how they are utilized. Without question, issues surrounding deploying the monitoring devices in public venues would generate a high level of concern.

One could imagine issues the use of these devices may cause. An example might include a medical privacy issue where the use of these devices may alert to small doses of radiological material residual from an individual's medical treatment. An "alert" on a package or backpack causing the item to be searched, leads to further search and seizure concerns. Educating the public about the technology and the devices and their uses for public safety is a must. As we move into the future, improvements of existing technology will result in fewer incidences of false positive and false negative reactions, which will aid in the public acceptance as is once did with airport x-ray scanners and baggage screening devices.

Implementation Planning

For law enforcement to successfully implement a CBRNE Sensor Management System, we must carefully assemble an implementation plan. Citizens who may be affected by the use of these devices need to be involved in the plan, and the agency needs to be responsive to issues raised from this process. We must open lines of communication early on in this process with as many stakeholders as possible.

It is critical law enforcement agencies consider implementation of CBRNE Sensor technologies to balance the benefits with the individual rights against unwarranted

intrusions. First steps in this process require that the law enforcement agency review the strategies and determine the best course to take for that agency. The Police Chief, on recommendation from staff, should make local elected officials aware of the direction the department is heading with this program. An overview of what can be expected should be part of this informational discussion. Assuming there is no resistance to the formation, the Police Chief should consider developing a steering committee, comprised of citizens, business leaders, and police staff, to oversee a monitoring process that includes not only the annual report to the City Council, but a complete auditing process evaluating the effectiveness of the program. Should the decision be made to move forward with the new technology, it is recommended that the following steps be considered as part of this plan:

Develop polices and procedures for use, utilizing Internal Stakeholders.

Goals and Objectives for use of WMD Sensors

- Define who is authorized to use equipment
- Who must be notified of use
- Identify who is responsible for maintaining records and completing reports on use.

Involve the community, service clubs, business groups, and stakeholders.

- Identify personal privacy concerns that will arise from monitoring.

- Gauge the level of acceptance and understanding of how the system is intended to work. Involve the groups in all aspects of project to attain comfort level.

Identify and Obtain Funding.

- DHD Grant money should be pursued for this program
- Donations from businesses as appropriate
- General Funds if necessary

Develop public information program specific to the use of WMD Sensors

- Hold informational meetings
- Use Department WEB site to post applicable information on this topic
- Display signs at the entrance points to all public facilities and venues where the devices will be used
- Establish Departmental point of contact for questions about the program.
- Establish protocol for filing citizen's complaints about the use of the devices.
- Publish results of the yearly evaluation of the program.
- Add a WMD Sensor component to the training that takes place in the Disaster Preparedness and Neighborhood Watch programs.

Deployment and Response

As with any major event or incident chain of command issues are sure to arise. Most agencies have utilized the Incident Command System ICS[6], which works exceptionally well when all the players are from the same community, and have the ability to train together on a routine basis. A release of CBRNE would most assuredly require the response of many different agencies. This type of response means the players will be coming together for the first time, thus a seamless transition must take place. Most agencies however should be well on their way to training staff on the National Incident Management System model NIMS[7] which was developed so responders from different jurisdictions and disciplines can work together to better respond to natural disasters and emergencies, including acts of terrorism. With the proper command structures and training in place the agency will be able to seamlessly blend the different organizations and agencies in a pre-designated manner. This structure will also aid in the need to iron out command related issues well in advance of an incident. This includes a well-defined, centralized decision making process utilizing the unified command system to assign resources and responsibilities for a smooth and effective delivery of services.

As each of these agencies respond, teams comprised of law enforcement, emergency services workers, fire, hazmat, and explosives experts will work together to resolve the incident. The Office of Emergency Services (OES) in each state may want to consider the purchase and loan of CBRNE sensor equipment and technology for use at events in the smaller communities, which may not be able to handle additional financial burdens. When dealing with CBRNE related incidents, decision makers must do their homework to understand each other's roles, protocols, procedures, and overall

[6] **Incident Command System (ICS): http://training.fema.gov/EMIWeb/IS/is100.asp**
[7] **National Incident Management System (NIMS): http://www.fema.gov/emergency/nims/index.shtm**

capabilities, and to ensure their respective communications capabilities are interoperable with one another to optimize the work of all aspects of a joint public safety response.

Program Monitoring – Tactical Concerns

Aside from the obvious response related concerns, the CBRNE devices are only going to be effective if the decision makers can monitor the devices from a remote location, once deployed. Portable, wireless sensors capable of being rapidly deployed and monitored from mobile or fixed command post are critical for success. Monitoring locations can receive real time information readily available to incident commanders who will be tasked with making the call as to "how" we will respond to the CBRNE sensor alert. Computer software working in conjunction with the sensors can provide "plume modeling"[8] to give commanders an idea range and direction should these devices be detonated. Evacuation decisions can be made prior to a device being detonated, thus putting emergency responders ahead of the curve which will in turn save lives.

Short-term concerns when deploying CBRNE sensors include the need to seek better technologies to better determine the validity of a sensor reading, prior to taking drastic action. False readings from sensor devices may lead to public distrust as well as unwanted pressures from local government officials, and may cause Law Enforcement leaders to second guess sensor information, leading to a slower response time, and potentially more injuries or greater loss of life.

Program Monitoring – Strategic Concerns

---

[8] Plume Modeling: Software designed to track and predict the atmospheric dispersion of hazardous material releases.

The overall accountability for using CBRNE Sensor devices rest with the Police Chief, and thus clear concise policies and procedures must be in place. Moreover, training on the use and deployment of the devices must meet the needs of the end users. Without this foundation in place, we cannot properly evaluate or hope to effectively monitor the program. CBRNE Sensor programs should reside in a specific area of the department where deployment and use can be consistent and monitored for effectiveness. Oversight of the program should reside at the senior management level. These individuals should be charged with not only monitoring the program, but also evaluating and reporting on the program as well. This should include quarterly reports that are directed to the City Council and are made public as part of this process. As part of the evaluation process, survey data should continue to be tracked and used to demonstrate any positive/negative public sentiments towards the project.

Conclusion

Implementation of a CBRNE Sensor program should involve careful planning. With many new devices coming on the market, agencies must determine their specific needs and level of protection necessary to accomplish the objective. Proven technology that has been field tested and deemed reliable by other law enforcement agencies should be a goal. Site visits to agencies using CBRNE Sensor devices is highly recommended. Once the agency has identified their needs and desired level of protection, a well thought out plan to move the project forward is a must. As with any undertaking of this magnitude, if the agency takes the time to develop the plan, this will reduce the stress levels of both the agency and the community served. One of the keys to making the plan

work is realizing that what works in one community may not work in another, meaning that hardware designed for one application may not be suitable for another. Implementation plans dealing with policy and procedures in one community, may not meet the needs of citizens in another community. Regardless, an end-to-end strategic plan that involves all stakeholders is a must.

The decision to purchase and use WME sensors will not completely solve or protect our citizens in 100 percent of the situations possible in the unknown future. Law Enforcement embarks on a new mission with the implementation of these devices. Rather than bringing crime prevention tips and tactics to our individual citizens in hopes of their eventual use, we are in fact now taking our own medicine and applying crime prevention tools community wide. WMD Sensors are the locks, alarms, and personal security measures of the future.

Scott Trudeau is a Lieutenant and 22-year veteran with the Livermore (CA) Police Department. Scott serves as a Tactical Commander and Emergency Operations Manager for his department. Lt. Trudeau is currently conducting a research project on the use of CBRNE Sensor Technology for law enforcement use in the Incident Command situations, while attending the California POST Command College.

SOURCES

1. **Levenson, N.G. 1995. *Safeware*: System Safety and Computers. Addison-Wesley.**

2. **Sandia seeks commercialization partners for hand-held chemical analysis and detection system."MicroChemLab" device serves as homeland security tool for first-line responders and offers variety of other applications: http://www.sandia.gov/news-center/news-releases/2003/mat-chem/chempartners.html**
3. **Sandia Sensors Guard D.C. Labs protect D.C. Metro: http://www.ca.sandia.gov/news/2003-news/030316news.html**
4. **Sandia Labs: http://ca.sandia.gov/news/2004news/080504news.html**
5. **Computer World Magazine: Feb. 2006 Super Bowl security to use sensor fusion to fight WMD threats. Todd Weiss.**
6. **Incident Command System (ICS): http://training.fema.gov/EMIWeb/IS/is100.asp**
7. **National Incident Management System (NIMS): http://www.fema.gov/emergency/nims/index.shtm**